Watch out for these malware scams

infotextmanuscripts.org/djetc/dj-watch-out-malware.html

What should you not do if you receive a suspicious e-mail? Do NOT click a link, any link. Ignore that advice at your own cost. I did.

Last month, I wrote an article about the latest Yahoo! password theft scam. That was the latest then, now there is another. Below is an edited message from the moderator of the Lewisham Freecycle Group. Before you read that though, read my latest hard luck story.

They say bad luck comes in threes, and that week it did for me: first, the new webcam I bought was not only bargain basement, it came with some unwanted non-optional extras; then my scanner packed up – I had literally burned it out building two quite large on-line archives. Then my computer started doing strange things shortly after I wrote the above article.

Okay, let's deal with the webcam first. I was doing some maintenance on one of my websites when I noticed something odd, hovering the mouse over the word "Menu" on one page, a link came up. Hmm, I don't remember putting a link there, I thought. I contacted my host, and received a prompt reply – as ever – to the effect that I should read the terms and conditions for my free account. I replied that I have a paid account. Oh yes, you have. That was when alarm bells really rang.

I won't name the software concerned, but before you buy any software – even over the counter – do some basic research on the company and the product. That problem was solved by reinstalling the webcam using different software.

Now to the big one, as I pointed out in my previous article, if you click the link concerned it will take you a fake website. DON'T CLICK THE LINK concerned, do not EVER click any link in any suspicious e-mail.

The following day I noticed my machine was doing things it shouldn't, so I ran some basic tests. Then an important file disappeared: msconfig.sys. I also ran my anti-virus software; I use AVG, the paid version, which is one of the best or maybe even the best around, it found nothing, so the next morning I phoned AVG and was put through automatically to a company called Techvedic. The guy I spoke to was obviously in India, but this turned out to be a case of outsourcing that was worth both the time and the effort.

After taking control of my machine he told me the bad news, someone else had taken control of it. He indicated a point of presence in Japan, yes Japan, and did some basic stuff to ensure that no further illicit access was obtained or damage done. I was lucky, he said, because this crook could have trashed my machine or done anything he wanted; fortunately he was only apparently after data like passwords – which I don't keep on my machine, and which you shouldn't keep on yours.

Then he told me the really bad news, my Windows XP set up had been destroyed, and I was lucky the machine was still working. He said they would have to rebuild it from scratch and replace XP with Windows 7. Then he said can you click here and enter your debit card details. This is really gonna hurt, I thought. It did, to the tune of £131.79. I wasn't sure I had that much in my account. I didn't, so I said I would go to the bank and pay in a hundred pounds. He said he would continue working on the machine in the meantime.

Fortunately, my bank is a short walk down Venner Road and into Sydenham Road. I paid in the money, came back, and my card was still declined. As he continued, I returned to the bank only to be told there was an "issue" with my account, and I should contact someone at the help centre on the internal phone. Uh oh, I thought, what else has this creep in Japan done?

After a half hour plus wait I managed to get through only to be told the issue was with Techvedic, its payment centre was in Panama. Truly, we are living in the global village. I sorted that out, returned home, and the problem was duly sorted for me. I thanked them and got back to work.

Then I noticed that my C: drive was write-protected. I sent an e-mail to Techvedic, but received no response. Having taken my money they were not so easy to contact, so I transferred my current files to the D: drive, and the following day, the C: drive was okay again.

It was only a couple of days later that I heard from Techvedic, a woman who spoke like an auctioneer on steroids. I didn't get much sense out of her, but thanked her all the same. To be fair though, these guy certainly knew what they were doing; they also spent four hours or so totally rebuilding my system and installing Windows 7, and gave me a one year on-site guarantee.

Although this misadventure left a hole in my wallet, that will be underwritten by my collaborator on the archive projects, but be aware, you may not be so lucky, so learn from my mistake. Don't click any suspicious link, the crooks may have a second string to their bow.

What really annoys me about people like this is that someone who has that degree of computer literacy and sophistication does not need to resort to criminality to make a good living.

Now here are a few other things to look out for. Shortly after the Techvedic guy had sorted out my machine, I tried to download a large attachment from my e-mail only to receive the message below – see the first scan.

We're upgrading BT Yahoo! Mail 2013

BT Yahoo! Mail

What you need to know

Dear Customer,

We've got a better version of BT Yahoo! Mail. It's lots easier to use, you can hang onto all your contacts, folders and messages, plus you get:

- faster email
- the latest spam protection
- unlimited email storage

What do I need to do?

If you use Internet Explorer 7, Firefox 3, Safari 4, or Chrome 5 or newer, you should upgrade now.

Click Here

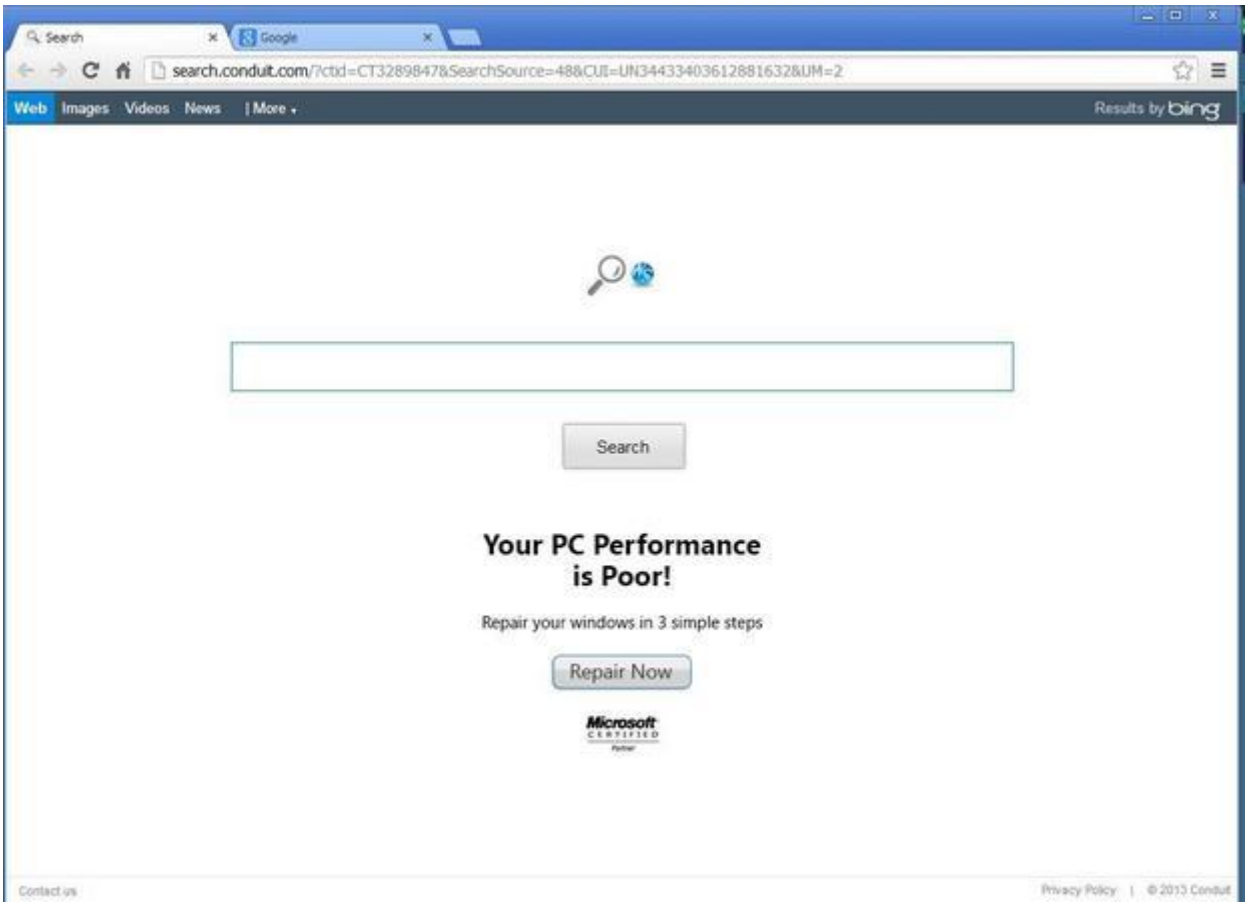
Thanks for choosing BT.
Warren Buckley
Managing Director, Customer Service

A phishing e-mail; this is NOT from British Telecom or Yahoo!

I was a bit suspicious of this so decided not to install this software. I contacted both Yahoo! and BT Yahoo! but the abuse@ address of the former sent me an automatic response which told me to report the issue using the (non-existent) link below, and BT ignored me. I checked out the website of InboxAce, and one or two scam notice boards. It appeared to check out, but I was not satisfied, and the next time I tried to download a large attachment, I did not have the same problem. So my advice is give InboxAce a miss; reputable companies don't need to resort to such subterfuge. How and why this happened with that particular download I'm not sure, but it doesn't appear to be anything on my machine.

Don’t be fooled. There is NO such compulsory update from Yahoo! or anyone else. Give InboxAce a miss.

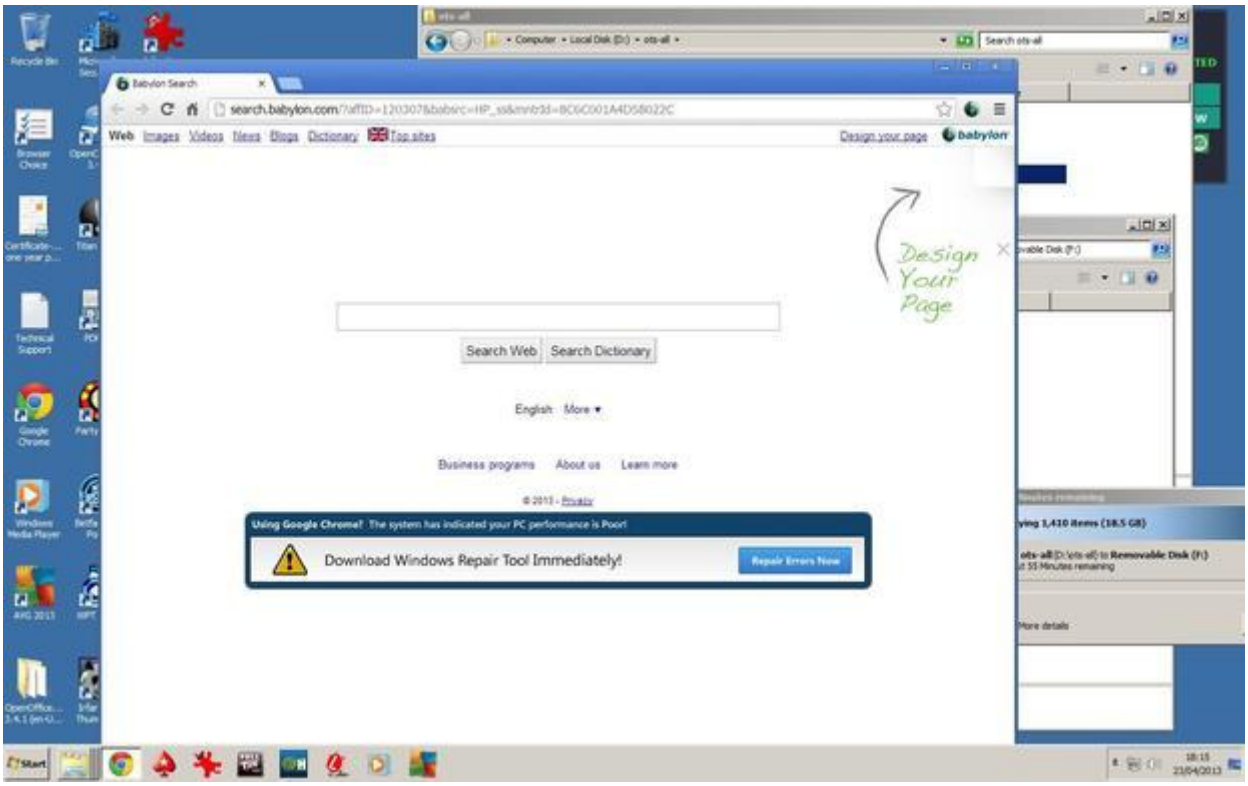
Another scam to avoid is searchconduit, which seems like a regular search engine. You have nothing to gain by using it, and could lose a lot, so give it a miss. Don’t be taken in by the message – see screengrab below – and if it does creep onto your machine by the backdoor, get rid of it fast.



Give Searchconduit a miss; your PC performance is not poor, so don't click the link.

Finally, there is Babylon, final screengrab. Again, don't click the link because there is nothing wrong with your computer, although there might be if you are taken in by these scam artists.
Very important, with the above and some other malware and rogue sites, don't click the link and don't click the cancel button either. There is one that tells you you are the 100,000th visitor, click here for your prize. You haven't won anything, you can't win anything, so don't click the link and don't click the cancel button because it is not really a cancel button. Close the window and seek help. Even if you have the best up-to-date anti-virus software, once you invite these scam artists onto your machine, there is little if anything that can be done to protect it.

Below the screengrabs is the message I mentioned earlier from the Lewisham Freecycle moderator. Be aware that if you use Yahoo! or similar groups you may likewise be targeted, again, don't click any link you think is suspicious, and if in doubt, err on the side of caution.



Babylon is another scam search engine. Don't click the link, don't click anything, close the page and get rid of it.

****

To all Lewisham Freecycle members:

Yahoo groups are still being deluged by SPAM posts.

This is a Yahoo problem, not one that Freecycle has control over.

Some members' email accounts have been hijacked and SPAM sent out to people in their address book including the Freecycle posting address...Please keep your anti-virus software updated on your computer and run a full virus scan now and again. Passwords should also be changed to something secure from time to time. You may also need to check your email account settings and disable the 'Out of Office' reply as that may have been compromised...Yahoo accounts are being attacked via a cookies loophole in Yahoo. Owners of compromised accounts need to sign out of Yahoo to disable the cookie, then clear the cookies and change passwords.
Changing the password alone will not be sufficient.

****

[The above article was first published May 6, 2013.]